TAC-TC January Monthly Meeting

Meeting Date:	**Feb. 6, 2023**
Time:	**10:00 AM US EST**
Purpose:	**TAC TC Full TC Meeting**

Attendees:

Name	Company	Role
Maroney, Patrick	AT&T	Voting Member
Thompson, Dean*	Australia and New Zealand Banking Group (ANZ)	Voting Member
Casey, Tim	Cyber Threat Intelligence Network, Inc. (CTIN)	Voting Member
Ginn, Jane	Cyber Threat Intelligence Network, Inc. (CTIN)	Secretary
Hohimer, Ryan	Cyber Threat Intelligence Network, Inc. (CTIN)	Chair
Schifilliti, Francesco	Cyber Threat Intelligence Network, Inc. (CTIN)	Member
Mavroeidis, Vasileios	University of Oslo	Chair
Zych, Mateusz	University of Oslo	Voting Member
Graham, Byron	US FBI	Visitor
Smullen, Scott	US FBI (on behalf of)	Visitor

* Will View Recording

Agenda:

- Overview of Progress -New Members
- Discussion of OCA CASP event
- Overview of CACAO

Transcript

This transcript was computer generated and might contain errors.

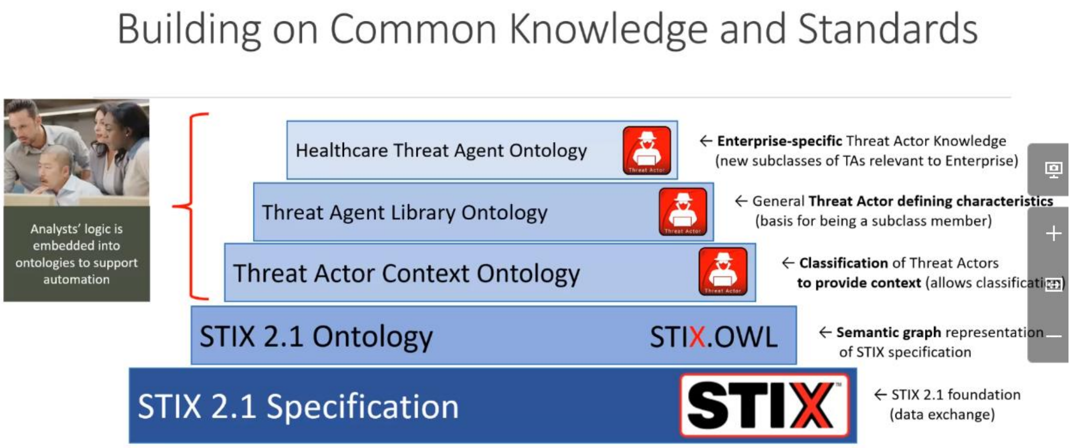
Ryan Hohimer: So today's agenda is really going to be simple. I want to go overview over what we're doing. I kind of anticipated some guests this morning that don't have the context of where we have been and where we're going. I want to go over the January accomplishments, and I want to reiterate that. We've got a new adapter in my firm semantic Arts. So the first part of this is just going to be what is it that we are trying to do here at the TAC TC So to give you the Baseline, that the real fundamentals of what we're doing in Tac is based off of the sticks exchange language. using that as our foundation we

Ryan Hohimer: created a sticks ontology in other words as tightly bound representation of this exchange language. which is very similar to a

Ryan Hohimer: it is not exactly but it's similar to A property graph in other words, it has actual. instantiated relationship objects in the sticks specification, but we have moved that to a semantic graph and represented the exchange language as an ontology. And then on top of that we've extended that. With the work of this group. Extending the sticks ontology with the actor context ontology. So, this allows us to subclass a threat actor into the types of threat actors that are appropriate for the investigation type.

Ryan Hohimer: The first use case that we took on for the Intel Corp, we built upon the actor context ontology there. tradecraft their interpretation of what a threat actor was for the Intel Core, so We extended the tac ontology with the threat agent Library. And then to prepare and show that this was extensible to other industry sectors. We actually did a demonstration for the Borderless Cyber Conference.

Ryan Hohimer: We did it a use case just a demonstration on how this could be applied to the types of thread actors that were involved in the healthcare industry particular. We did an emphasis on the Curious healthcare worker.



Building on Common Knowledge and Standards

Analysts' logic is embedded into ontologies to support automation

Healthcare Threat Agent Ontology ← **Enterprise-specific** Threat Actor Knowledge (new subclasses of TAs relevant to Enterprise)

Threat Agent Library Ontology ← General **Threat Actor defining characteristics** (basis for being a subclass member)

Threat Actor Context Ontology ← **Classification** of Threat Actors **to provide context** (allows classificati

STIX 2.1 Ontology STIX.OWL ← **Semantic graph** representation of STIX specification

STIX 2.1 Specification STIX ← STIX 2.1 foundation (data exchange)

Ryan Hohimer: Okay, the idea behind building the threat actor context ontology is to get a better representation of threat actors and the context within which they perform and this is been addressed by our industry in terms of the Pyramid of pain. So this triangle there are things that we can do.

Ryan Hohimer: Are to address threat actors that are at the easy level, We can look at indicators of what types of IP addresses they might be coming from or the type hashes of the different types of viruses that they might be using the malware that they might be using. So when we think about the easy things that we can do that are more along the idea of cyber hygiene, we can start looking for hashes and ipses and frequent domain names that they're using but as we progress up this pyramid of pain the more we know about a threat actors techniques tactics and fatigue procedures and the more that we can defend ourselves against that the tougher it is for them to deal with our Institution

Ryan Hohimer: or the better that we can recognize in the types of things that those threat actors are doing. What is true. is that this pyramid of pain does definitely address. the context of thread actors, but if you think about it Who are the adversaries of the thread actors they adversaries of the threat actors are the Enterprises the individuals that they're trying to? profit from and so if we invert this pyramid of pain from the perspective of the threat actors as the Defenders have got the same set of

Ryan Hohimer: context or the same context their ability to penetrate their ability to be effective against us is inverted in this way and really that forms this Battleground that's between us. In terms of the interactions and the exchanges that we might have with the threat actors. And so this is out for years and years. This is reminded me of and it's really an overdone analogy, but the sunsuit quote if your enemy and yourself, you need not fear the result of a hundred battles, but if you don't know the enemy or you don't know yourself, you're in trouble.

Ryan Hohimer: So that brings us to why we are doing what we're doing right now. We're trying to prepare. For the cybersecurity automation Village the plugfest that's about to happen. I'm just reminding those on the call that we can now go and register for the plugfest. This is not strictly and Oasis member thing this is anybody can participate in the plugfest. So I'm just bringing to attention the Eventbrite invitations that's here for everyone to participate in and so early to send out an invitation

Ryan Hohimer: in that plan, I didn't know it's So what did we do to get prepared for the plugfest? So we've developed the build process to merge the different ontologies files that There's more than 52 at this point. I didn't write down the exact amount, but we've in the past.

Ryan Hohimer: Month actually the last couple of months we have. Been able to take and merge all of the ontology files of the sticks and Tack ontologies. And the talentology but the sticks and Tack are the two ontologies that this group is developing into a single file. I've been able to use the OBO. This is the open biologics ontology robot utilities in an automated fashion put the 52 files into

Ryan Hohimer: a singular file. this just makes it so much easier for an adopter for a user to deal with the tack ontology if they've got to deal with 52 plus ontologies. They've got to make sure that they're configured properly and the rest of it it's a barrier to entry that's one that we wanted to remove. So in the beginning, several years ago when started did we have some odd plus files. They were all in their own namespaces. to manage very difficult to use. So at this point in time, we've brought it to a point where it's extremely easy. There's a single name space and it's in a single file.

Ryan Hohimer: We're able to translate second thing we've got on our accomplishment list is we're now able to easily translate sticks 2.1 Json. This is just six data. So we can take a stick Json file one run it through our code that we've developed.

Ryan Hohimer: shift that from being a sticks document into an rdf formatted file. So this allows us to take sticks documents and see them as knowledge graphs. So once we've converted that we import That sticks filed those facts. Into a Knowledge Graph that's governed by our ontology. So we were able to develop that into one file. We take the one file we import the facts that we've just converted and that gives us a knowledge base that we can view in Base Knowledge Graph databases the platforms such as star dog gravity B.

Ryan Hohimer: I've been working primarily with allegrograph for the last. couple of months simply because I have a relationship with the company itself and their visualizations are good. They do their visualizations and growth.

Ryan Hohimer: So we've converted miters Framework from the sticks Jason representation and loaded it into our knowledge graphs. This would be an example of knowing the ttps basically of a Bad threat actors. We've also in the process. I have not completed it yet, but I'm very very close converting that cve data the common vulnerability enumeration data. with our code into the

Ryan Hohimer: it's actually National vulnerability database is not provide it in sticks format, but they provided in their new format and so I've just about completed a Code Sparkle anything code to convert that into the rdf? Knowledge Graph so that we can use those cbees with knowledge of the ttps from miter attack and are threat actors in an environment. I'll talk a little bit more about that. In future work. We did not get this accomplished in January. I'm hoping that in the next two months prior to the plugfest that will be adding the CTE data.

Ryan Hohimer: To the mix so that will not only have The ttps through miter attack, but we'll have the cpes of all the platforms that are usually in the Enterprises environment. and then we'll be presenting Some visual queries with Gruff. we extended out a

Ryan Hohimer: a keynote speaker request to Jane's Osman from allegrograph and he is going to be one of the keynote speakers at the plugfest and in that interaction with him. he's been helping me come up with some visual queries in representing that the typical questions of analysts Within the cybersecurity domain. So this is kind of a new interaction that I hope to follow up on and make the most of for the next couple of months. So, what does that look like? It means that we've got miter attacks framework?

Ryan Hohimer: You can see that not only have we taken miter attacks six data. We've converted it into a graph and we're able to work in a graph database as you're seeing here. Again, I just put this sun Sue's Art Award down here to remind us both. on the defender and the attacker side that this is a spider attack as a matter of knowing that top or the tip of that pyramid of pain. We've got to understand what the adversaries techniques tactics and procedures are. And if you think about the inverse what are the business processes? what are they? procedures

Ryan Hohimer: and the things that we must do in our business to be successful or within our Enterprise and so might as attack framework, I believe addresses both knowing yourself and knowing your enemy. we've also accomplished the 90% of loading the common vulnerability enumeration into the tech framework and again, why are we doing these?

Ryan Hohimer: Common vulnerabilities are the vulnerabilities that we have defects in our software products. And they're the things that are targeted by the thread actors. So knowing the cbees, knowing a matter of ourselves understanding where we are vulnerable.

Ryan Hohimer: and then of course understanding the enemy which enemies have got the capabilities of actually exploiting those vulnerabilities. for the plugfest I wanted to kind of lay out this mapping.

Ryan Hohimer: Keven and I had been talking over the last several months about open CTI and the possibility even in the October time Of 23 we were talking about Maybe we can pull together a graph back in to support open CTI.

Ryan Hohimer: that the resources that we have in the TAC and the m and the time frame that we have to function in it made more sense from our perspective that we not try to work on the open CTI tool itself, but to continue to work at flushing out and making more capable the attack on solid the sticks and Tack ontology and so The idea here is that we can take the sticks output from open CTI. We can feed that through our software to convert it into rdf. And then we can take that rdf and work with it within a platform. And we can use that. Platform to organize the relationships between the objects.

Ryan Hohimer: In the current Knowledge Graph we have and perhaps even use as we did with the Intel Corp data and ontology provide automated inferences about threat actor typing. once yeah

Patrick Maroney: I intend with the interoperability Villages presuming Microsoft is going to give us the Azure resources to stand up open CTI. And so there should be again barring any breakdown and the timeline here. There should be an instance of open CTI available for us to prototype and go to an integrate with. Those are fairly straightforward. It's not going to be a fully production ready fleshed out version, but it will be sort of an out-of-the-box Docker container. So just in your planning Please be aware that is one of my key Target objectives for the blood Fest in April. Likely not going to happen before the Prep 2 blood vest over.

Ryan Hohimer: right

Byron: Hey, and can I jump in just add a little something to that if you're gonna utilize open CTI just as an FYI, we have been adding some development on sticks objects that are not in the Oasis Library specifically the threat actor individual. And that has been merged as part of the main branch code within I want to say open CTI 5.11 and newer. So that just says that object is going to be in there. That's not in. part of the Oasis ontology

Ryan Hohimer: So it may be I'm just reacting to both Patrick and was it Byron? And I'm just reacting to the extending of the tac ontology with a new type of the threat actor individual

Ryan Hohimer: We've been prepping to do exactly that so.

Ryan Hohimer: we can incorporate that I think before that the plug test just to So if we come up with the use case that extensively uses the individual then it can be part of this chain. I'm talking about right now. It should be fine. Okay, yeah.

Jane Ginn: Ryan, can I also give right Byron and Scott a little bit more context around what we're trying to accomplish with the Plugfest?

Ryan Hohimer: Yeah.

Jane Ginn: So the Cybersecurity Automation Subproject (CASP) the Open Cybersecurity Alliance, which does not restrict itself to members of Oasis. So it's an effort to reach out to the broader community and involve some of the companies that are building product in this area and doing work in this area not only companies but think tanks academic institutions government agencies Etc and we are hoping to provide a platform to show interoperability between several of the security related technical committees within Oasis. including cacao

Jane Ginn: Csaf, which is the technical committee that is a common framework for vulnerability analysis The sticks and taxi standard which is part of the Cyber Threat Intelligence technical committee plus some of the other sub-projects including Kestrel. Which is an automated threat hunting capability. Open C2 which is also a mechanism lead largely by the NSA for automating network actions what else am I missing? Kestrel stick shifter, which is like an elevator for sticks data objects And then anyway, you can see that it's aimed at bringing together a lot of work from a lot of different threads all together so we can start to look at the interoperability between all of these different threads.

Patrick Maroney: And the posture attribute collection and evaluation, Otherwise known as PACE. The links to that LCA put them in the chat.

Jane Ginn: Thanks.

Ryan Hohimer: If you can see this is a Venn diagram that I really threw together in a moment. So it isn't as accurate as I would like to be but one of the things that it does. is this talks about the breadth of the domains within the cybersecurity community and Tac is just one small bubble in a larger set of domains that we need to be aware of and Mateos and mask and talk to you about some of the other adopters that we have in terms of agencies and European agencies and institutions that have started to adopt the attack the

Ryan Hohimer: Tac ontology, but close to my heart because I'm one of the Consultants with semantic Arts is that their looking at the work that we've done with Tac over the years and starting to incorporate that in what they call their?

Ryan Hohimer: just cyber so actually kind of the opposite we around semantic Arts is developing an upper ontology. of the cybersecurity community of which one of the domains

Ryan Hohimer: Within that upper ontology. Is that threat actor context ontology. So on that previous slide in order to be effective at developing an application in cybersecurity.

Ryan Hohimer: One has to be familiar with all of these domains. And so at semantic Arts. We want to adopt the work that's been done in Tac. as one of the many different domains that are covered by this upper ontology.

Ryan Hohimer: so Pat Maroney and I have been friends for years and we've been involved in multiple efforts to Such an upper ontology my firm myself particularly are taking the spearhead to try to develop another upper ontology. That's easy pragmatic useful for the community. So I just wanted to Let you members of the TAC. know that semantic Arts is developing an upper ontology which one of the seven ontologies will be Tac.

Ryan Hohimer: this is a very old slide, but I thought it was appropriate since it's gotten Byron were on line or possibility going to be here with this morning the extension of Sticks data objects in Tac is what we built. It's how we configured. the sticks and Tack ontology. it's hierarchical adding an additional sense and extension to a stick domain object is rather quick and easy. So instead of extending vulnerability like I'm talking about here.

Ryan Hohimer: We can easily do that with thread actor and have a threat actor individual and Associate the very specific attributes of an individual threat actor that you and your tradecraft have identified. So it isn't just a matter of saying hey, I'm going to tag This Thread actor as an individual threat actor. We can actually specify the attributes that you believe in your trade path make that thread actor specifically an individual with the individual's capabilities as opposed to a group or

Ryan Hohimer: yeah, okay, so I'm going to stop sharing this is basically The culmination of what we got done. in January, is that we made significant progress towards prepping for the Casper plug threat Fest and I cannot see who has hands raised any of that Maybe if I change views now.

Jane Ginn: So I'm wondering if we can shift gears here and let Vas and Mateusz talk about the work of CACAO?

Ryan Hohimer: Absolutely.

Jane Ginn: Scott and Byron about the work they've been doing in cacao because I think that may be of interest as well. are you at a place where you can turn on your mic and speak? I know sometimes you're on a train.

Vasileios Mavroeidis: Yes. Yes currently so high Byron and nice to meet you and welcome.

Vasileios Mavroeidis: So regarding a cacao so it is a technical committee. So we developed a standard and now we have started also developing some tools that are basically sponsored by us and they are under the OCA umbrella. They open cyber security Alliance umbrella, which also associated with Oasis, but basically making the long story short, so we've cacao we aim to achieve with playbooks what the CTI Community achieved We Stand us like sticks and taxi, so we have the need to be able to better formally describe defensive tradecraft. So basically an example would be right. How do we respond to an incident? So we are very good in creating, detection engineering and coding.

Vasileios Mavroeidis: Thin sticks and the context around that but where it was about, the show know what sticks was doing very bad because the course of action object basically was a stub object that you could include something only in prose. So we create this workflow format at the end of the day what we able to have is Format that can be consumed by any kind of solar system for Pure automation. Right? But also you can couple this playbooks with cyber threat intelligence. This is it more or less. there is a specification itself into inversion 2.0 it's a robust document. So yeah. I'm not sure you have heard about cacao or

Byron: Is Cacao the Korean chatting application you're just talking about. Is that what you're talking?

Vasileios Mavroeidis: To know so cacao stands for collaborative automated course of action operations. And basically this is an oasis standard and it's basically standard that allows you to create cyber security playbooks. So you can see this as something that cyber threat intelligence gives you context about, the adversary but security playbooks will give you the context regarding how you respond to this adversary specific intrusion set campaign, right?

Vasileios Mavroeidis: So we didn't have this format, So if we no let's regarding how do we respond to something? And this is a workflow right or a security Playbook. We didn't have a common format to exchange this playbooks in addition to cyber threat intelligence. So the most known concert associated with security playbooks plus workflows is short platforms security orchestration automation response platforms and all of them come with their own proprietary notation when they design playbooks. So when you want to exchange this playbooks right for the sake of automation, unfortunately would be able to consume this Playbook only if you have the same solution So maybe this is coming from Palo Alto. Let's say so you need to have a palv Alto system to be able to consume this label. So the whole point was to make security playbooks interoperable and last cerebral.

Jane Ginn: I'll also add that vas and Mateos have developed. An online tool that they've shared with the community. It's on GitHub right now Mateus in our situation where you could share your screen and show them your roaster tool.

Mateusz Zych: That's a good question.

Mateusz Zych: I think so, but just super briefly.

Jane Ginn: Okay.

Byron: Hey guys.

Jane Ginn:

Byron: Thanks for contextualizing. The cacao is listening to you. But having lived in Korea for a while. I'm so used to the Korean cacao chat platform. I thought maybe it was some relationship to them. But thanks for contextualizing that for me.

Vasileios Mavroeidis: Absolutely.

Mateusz Zych: Lost you want to still talk or?

Vasileios Mavroeidis: I mean I can do that.

Mateusz Zych: It just showed the screen.

Vasileios Mavroeidis: Yes web application that we have a open source, Casey it's like sticks right? it's a taxonomy, right? We cannot call it an ontology that allows you to connect stuff together to make some sense out of this stuff. But unfortunately this stuff I are encoded injection. So this is not very easy for humans to create the web application so we can actually generate security playbooks which is basically a set of actions right for the purpose of Performing something. This may means the response with me. This may be random relation exercise. This may be threat hunting this may be something related to detection investigation analysis deception, you name it. So we have different Playbook formats. And then of course, the specification is a heavy document like the stick specification that allows you to put all these elements.

Vasileios Mavroeidis: Together but at the end of the day the difference between sticks and the cacao is that in account? You can create basically a workflow. So when you visualize it you go from one step to another step and you are expecting, something to inform you that the previous step was performed correctly, maybe some kind of output from one state from one step that's going to serve as an input for the next step, etc. Etc. So this is basically how short Solutions work. So in order to is The process of creating account playbooks you created this web application.

00:40:00

Vasileios Mavroeidis: Yeah, yeah. No, basically that's the workflow or…

Mateusz Zych: Yeah.

Vasileios Mavroeidis: security Playbook that the CISA published a while ago along with other workflows. For example incident response, for vulnerability management. So here description vulnerability response process this was a PDF document basically and we transpose these into Jason. So basically, you use the graphical interface to create the Playbook, just so the Jason, code, which is basically how you see what you see exactly in sticks when people sticks

Vasileios Mavroeidis: let's say that this Playbook was not just the standard operating procedure right about vulnerability management process, but it was the Playbook that the response to conference somewhere. You could take this Playbook, if you are FBI, you can digital sign it as FBI because the application has this functionality and the standard itself basically and…

Mateusz Zych: (showing demo)

Vasileios Mavroeidis: you could share it with cyber threat intelligence. So that could be for example some indicators when you identify this indicator, We are pretty sure that you been I infected by a conti and this is a step This is the process you're supposed to perform, either to mitigate or remediate. So then based on your maturity. You can either fully automate this Playbook. You can execute manually or you can develop something hybrid. So there are approaches now there is an open source orchestrator. It's working progress that happens this web application, as you see them we say around the glass thinking it's action step in each rectangular basically that connects with an orchestrator and based on if a step has been executed successfully or not. It changes to green or red, etc, etc.

Vasileios Mavroeidis: So this is let's say the front end of a short platform, but basically allows you to create the playbooks on the other hand. We can also export them and couple them with sticks. And cacos on standard. So we have created extensions for sticks not have extended the construction as the other sticks domain object and then it's not that we didn't in a way that you can basically change any kind of playbooks. This may be for example a docx document the PDF ansible playbooks, from a phantom from Splunk or call playbooks that are interoperable, but we made it also, Format agnostic, So not only better diagnostic pad for once.

Vasileios Mavroeidis: And Ryan you raise your hand, but your muted so we can't hear you.

Ryan Hohimer: Sorry, thank I appreciate it. I'm not hitting on all cylinders today. So is I know that earlier you had done the work to actually integrate this with the TAC and sticks ontology. So we had all of this at one point that was integrated is what would it take to validate that integration that you had on security playbooks is still valid and could we actually have that prepared by the time of the plugfest?

Vasileios Mavroeidis: Yes, so you're having above the extensions, So the extensions are fine.

Ryan Hohimer: Yes.

Vasileios Mavroeidis: So they are valid sticks to point one extensions. The schemas are okay, but I do believe that we could improve very presentation of the extension nevertheless. There are bus States right to use them. I do believe though because it was like a few individuals that supported this effort, we need to bring it forward to the city it see at some point and all of us agree on a common representation. There are no other words out there. So Johns Hopkins University and basically sign quotes now put that they are using the same extension but basically some properties removed means, they are not only required here. So some optional properties are not part of how they exchange their play.

Vasileios Mavroeidis: But the extension is the same. so It works nevertheless.

Ryan Hohimer: Okay.

Vasileios Mavroeidis: Don't forget it will be fine to share it through taxi server. Unfortunately Open CTI is not very granular Miss that you import object templates and then they appear in the user interface. So for open CTI, we would have to modify the back end models Etc. So it's not our best but at some point we may do it.

Ryan Hohimer: Thank you.

Vasileios Mavroeidis: So mending also with some other systems right now. This is the reason we were very keen with open CPI, but then it has some Challenges when we want to integrate some stuff and then because our priority world that we wanted to integrate collaborative instant case management system. We found this Irish food. Have you heard about This Iris collaborative instant case management to work in progress

Vasileios Mavroeidis: but still it has a connector with misp. So, it's not a big issue for us to transition from one platform to another since we have a python converter, right? We just need to create a pipeline and more resources, but It seems that with me It's open source, and it's a good collaborative platform considering also that the hive and the other components that are together with a hive some of them have gone under licensing schemes, and getting complex.

Vasileios Mavroeidis: I did the conversation, but at least I think it's good to know about this platform. It's under development.

Jane Ginn: Thank you That's great. Byron Scott do either of you have any questions given that We've been going through so many different things that we've been working on as a TC over the last what two plus three years.

Byron: There's a lot to digest here. So I think I would have to really kind of comb through this. I'm bookmarking sites and referencing them to other people in our team. So I think you guys have given us a lot to look at and…

Ryan Hohimer: Yeah.

Byron: stuff. It's Really just wanted to kind of also sync up, our efforts with your efforts and kind of align our thought processes Even Ryan some of the things you talk about. Regarding the threat actors and threat actually individuals we have on our platform if you get the open CTI, I want to say Five Dot 12 and newer it looks like probably 6.0 is probably going to drop here probably this month sometime. but in the threat actor individual we've Been able to kind of capture.

Byron: different properties, for us we care about identifiers obviously email addresses and user accounts that they would use but also from our perspective we actually care about, height weight eye color hair color that kind of stuff, if we're gonna go out and put handcuffs on people it's like we want to make sure that it's the right guy and so, having those things is important, but I know that I think some of the privacy laws in Europe make this a bit of a challenge and so I think there are features that you can kind of toggle that capability on or off so that you're not I guess in Jeopardy of looking at violating that information but for our case purposes and for some other regions, it's things that care about

Ryan Hohimer: So that makes perfect sense. to me, so there's a

Ryan Hohimer: there's a high level distinction between the types. of

Ryan Hohimer: Uses of these types of ontology. So what am I saying here? I'm saying that in some iterations. you're using a tool like sticks ontology not the exchange language, but the sticks ontology and the pack ontology the threat actor context ontology for two different purposes. One is for investigated purposes to work left of boom. I want to prevent what I anticipate might be coming. I don't necessarily have to absolutely prove that this occurred but I have to Intuit that a pattern is and process that might occur as opposed to another aspect is more the forensics aspect. Hey, if I'm gonna pull a trigger or I have to have actionable intelligence and the fact that I'm gonna pull a trigger or I'm going to arrest or I'm gonna fire an individual then

Ryan Hohimer: had got to have all the

Ryan Hohimer: Forensic evidence so that I'm prepared to go into a jurisdiction. So there's multiple context that have to be considered at even the upper level. so that as we start providing the capability to collect up all those attributes about it individual that we've done so in a matter of a way that It's going to hold up in a court of law. Is that make any sense to you guys? I mean There's definitely. That the type of activity that's going to happen out in the stock of an Enterprise and there's a type of activity that's going to happen. can be plugged into.

Ryan Hohimer: Action courses of action that are actionable intelligence that will hold up in a court of law. I think I'm babbling in my covid haze here. Sorry.

Jane Ginn: Ryan I see that Patrick has his hand raised and vast has his hand raised. So let's first go to Patrick.

Patrick Maroney: Hey Ryan, on your comments about the physical characteristic Etc.

Patrick Maroney: So I'm a very strong advocate for us not Reinventing any wheels or be creating any rings to rule other rings. So we're closely tracking the meme efforts moving mean so to the extent that that is something we could subsume or integrate from an ontological perspective. That would be the approach that wouldn't barge from doing some simple placeholders. But where you can because once you start bringing in other pieces, it gets very complicated. I've worked with the OMG effort to do the threat risk model which tried to merge dicks and mean XML back in the day. so for those characteristics and I'm not going to get into something the funnier humorous aspects of what mean can describe physically on an adversary. That would be the strategy over.

Jane Ginn: And I see Byron has to drop for meeting and…

Byron: Yeah.

Jane Ginn: Vas. You want to follow up by email?

Vasileios Mavroeidis: Yeah, of course. I mean we won't have enough time because I want to ask them basically how they have implemented that is it an open CTI? How did they handle the model? I mean have they used really formal sticks to point one extension because if you want to exchange in that via taxi, and they don't have extension is not going to work very well. So I just want to get all this information is something publicly available because you also mentioned the version that's coming out open CPI. And I inferred somehow that this is going to be part of the latest version so, all these information

Byron: Yeah, all of our contributions to this vase and everybody we are contributing to the main code Branch. So all the efforts that we're doing everyone's gonna benefit from us so you can actually go to the GitHub account, you'll see a lot of the contributors are directly from the FBI cyber division GitHub account. So if you download the latest version, you're gonna use and see what we're using and seeing so you'll be able to see it.

Vasileios Mavroeidis: and perfect

Byron: I think just one little thing that kind of Patrick was talking about that we've been dealing with lately is we're trying to figure out better.

Byron: The Alias function isn't really working for us very well. And so we're starting to kind of pivot and use user accounts which is an observable but we know that the Styx model doesn't really like, let's say intrusion sets using user accounts. And so we're trying to find a way of kind of associating those and those relationships with user accounts with the threat actors because the Alias function at least within open CTI just isn't really granular in the and kind of the Act of the threat

Byron: Group crosswalks from all the different reporting, Mandiant data. They all have their different naming conventions and they're not a one for one and even us in the intelligence Community. We could even more granular like North Korea is just broadly Lazarus group, but other people they kind of slice. Those into pieces based on what they see. m sorry. I would love to talk because these are really good discussions. I really like the words going Vice. Yeah, let's continue that discussion. I can probably Loop in one of our software Engineers that could discuss how we did the integration on the back end. Thanks for letting me listen in and please send me the invites for future meet up. really appreciate

Jane Ginn: Okay, and you guys I have to drop too. I've got a meeting starting now. So, thank you everyone. We'll see…

Vasileios Mavroeidis: And see you soon.

Jane Ginn: We'll set up the next working call for February.

Mateusz Zych: Thank you.

francesco schifilliti: Event. Thank you.

Vasileios Mavroeidis: Yeah.

Scott Smullen - CyD (Contractor): Thank you all very much. Ryan feel better.

Mateusz Zych: All right.

Scott Smullen - CyD (Contractor): Nice meeting you.

Ryan Hohimer

Adjourned Meeting

Reference Links:

TAC Ontology Architecture Specification:

https://docs.google.com/document/d/1ejdrBLzVrP-NgrZmHI9bN62EgishRIltq2f90_h5d3s/edit#heading=h.105543clms0k

TAC Technical Specification

https://docs.google.com/document/d/1ky1CAUDKpn3RddbCvvYGudctwL5LGi2SMs_fTKdpQ8w/edit#heading=h.gjdgxs

Semantic Web Re-Engineering Tool

https://github.com/SPARQL-Anything/sparql.anything

Meeting Link Terminated